Sun™ Crypto Accelerator 4000 Board Version 2.0 Release Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 817-6973-12
May 2005, Revision A

Submit comments about this document at: http://www.sun.com/hwdocs/feedback

Please
Recycle

Adobe PostScript

Contents

Sun Crypto Accelerator 4000 Board Version 2.0 Release Notes

These release notes describe known issues of the Sun Crypto Accelerator 4000 board. For the latest version of this document, refer to:

```
http://www.sun.com/documentation
```

For the latest patches, updates, and requirements, visit the product web pages at:

```
http://www.sun.com/products/networking/sslaccel/suncryptoaccel4000/
```

The patches listed in this document are available at: `http://sunsolve.sun.com`. Solaris Operating System update releases contain patches to previous releases. Use the `showrev -p` command to determine whether the required patches have already been installed.

Install the latest version of the patches. The dash number (-01, for example) becomes higher with each new revision of the patch. If the version on the web site is higher than that shown in this document, it is a later version.

If the patch you need is not available at the SunSolve℠ web site, contact your local sales or service representative.

Required Patches

The following table lists the required patches available for Solaris 10:

Note – Always check for the latest revision of the patch, -01, -02, ...

TABLE 1 Required Patches

Patch	Description
116781-01	Sun Metaslot Patch
118918-03	`libpkcs11` Metaslot Patch
118961-01	SunVTS 6.0 Patch Set 1 for SPARC platforms

Version 1.1 and 2.0 Software Contained on the CD-ROM

The Sun Crypto Accelerator 4000 Version 2.0 CD-ROM contains both Versions 1.1 and 2.0 of the software.

Caution – Version 1.1 is for Solaris 8 and 9. Version 2.0 is supported on Solaris 10 only.

The install script path is changed as follows:

For Version 1.1:

```
/cdrom/cdrom0/Sun_Cryto_Acc_4000_1_1
```

For Version 2.0:

```
/cdrom/cdrom0/Sun_Cryto_Acc_4000_2_0
```

The respective installation scripts are located in these directories.

Sun Crypto Accelerator 4000 Board Version 1.0 and 1.1 Not Supported in Solaris 10

The Sun Crypto Accelerator 4000 1.0 and 1.1 releases do not take advantage of the new Sun Cryptographic Framework provided in Solaris 10. Because of this, the Sun Crypto Accelerator 4000 1.0 and 1.1 releases are not supported with the Solaris 10 Operating System.

The Sun Crypto Accelerator 4000 2.0 release uses this new framework, and is available as a free upgrade to current Sun Crypto Accelerator 4000 users planning to use Solaris 10. Because the Sun Crypto Accelerator 4000 is an export controlled product, contact Sun Enterprise Services or your local sales channel to obtain the free upgrade. Additional information is available on the Sun Crypto Accelerator 4000 web page:

`http://www.sun.com/products/networking/sslaccel/suncryptoaccel4000/`

Migrating Keystores From Version 1.1 to 2.0

When migrating from Sun Crypto Accelerator 1.1 to 2.0, the encrypted keystore file is automatically converted to the format expected by the Version 2.0 firmware. This conversion is an irreversible process.

To use an existing keystore to initialize a 1.1 system in the future, a master key backup must be performed prior to installing the 2.0 driver and firmware. Both the master key backup file and the current keystore file must archived to successfully initialize a board with the current 1.1 keystore. By default the encrypted keystore file is located in the `/etc/opt/SUNWconn/vca/keydata/` directory.

Known Issues With the Sun Crypto Accelerator 4000 Software

Using `vcaadm` With AES and Metaslot Enabled

If both AES and Metaslot are enabled, and you use the `vcaadm` utility to initialize or zeroize the board from the system to which the board is attached, error messages similar to the following could occur at the end of the operation.

```
Initializing crypto accelerator board.  This may take a few
minutes... C_DecryptUpdate failed: CKR_DEVICE_ERROR
```

This operation completes successfully; however, the response output is not decrypted.

Workaround:

Disable AES by removing the `enable-aes=1;` line from the `/kernel/drv/vca.conf` file and reboot the system.

OR

Disable Metaslot in the environment that you want to use `vcaadm` as follows:

```
% METASLOT_ENABLED=false
% export METASLOT_ENABLED
% /opt/SUNWconn/cryptov2/bin/vcaadm
```

Bug ID 4850432 Link Down on First Plumb With IPMP

The board generates a link down notification on the first plumb when using IPMP. This causes the board to fail initially in an IPMP configuration. The failure is then cleared in approximately 30 seconds.

Workaround: Wait 30 seconds for IPMP to clear the failure.

Bug ID 4922816 Outbound IPsec Might Not Offload

Outbound IPsec does not offload if the hardware is newer than the Security Association (SA). If a Sun Crypto Accelerator 4000 board is configured in a system for in-line IPsec acceleration using existing SAs, the Security Association Data Base (SADB) must be reloaded in order to use the existing SAs. Reloading can be performed by rebooting the system or using the `ipseckey` utility. Refer to the *IPsec and IKE Administration Guide* for information on how to use the `ipseckey` utility.

`vcaadm` Lock File

A `vcaadm` lock file (`.trustlock`) is used to prevent overwriting of changes between two `vcaadm` processes. If the `vcaadm` utility is not shutdown properly, this lock file might prevent access to a trust database. If this issue occurs, you receive the following error message:

```
Lock file prevented read access to trust DB: Timer expired
```

Workaround: Remove the `.trustlock` lock file in the `${HOME}/.vcaadm` directory.

```
# rm ${HOME}/.vcaadm/.trustlock
```

Cannot Open Keystore Messages

If an attempt is made to use an initialized board without the correct keystore file present in the `/etc/opt/SUNWconn/vca/keydata/` directory, an error is reported to the Solaris Fault Manager Daemon (`fmd`). Messages similar to the following are logged in the message log each time a cryptographic operation is attempted on the board:

```
Feb  1 15:39:29 gost vcad[100810]: Cannot open keystore
/etc/opt/SUNWconn/vca/keydata/vca.8302c1bf420012a5: No such file or directory
Feb  1 15:39:29 gost vca: WARNING: vca0: Unable to load keystore vca
Feb  1 15:39:29 gost vcad[100810]: Failed issuing VCACTLFILEGET ioctl: No such
file or directory

SUNW-MSG-ID: SCA4000-8000-5V, TYPE: Defect, VER: 1, SEVERITY: Minor
EVENT-TIME: Tue Feb  1 15:39:33 PST 2005
PLATFORM: SUNW,Sun-Blade-1000, CSN: -, HOSTNAME: gost
SOURCE: eft, REV: 1.12
EVENT-ID: 3f9eac7d-de93-c177-ebe5-fb3626c2c607
DESC: The Sun Crypto Accelerator 4000 keystore file could not be loaded to the
card via the vcad daemon.  Refer to http://sun.com/msg/SCA4000-8000-5V for more
information.
AUTO-RESPONSE: The driver will attempt to load the keystore prior to performing
every cryptographic function until the file is successfully loaded.
IMPACT: The card will continue to function, but will be unable to perform
cryptographic operations using secure keys until the keystore file can be
loaded.
REC-ACTION: Restore the keystore file to the correct location.  Contact Sun for
support.
```

These messages are logged regardless of whether or not the keystore is needed for the specified cryptographic operation and can quickly fill the log file. To avoid this problem, the correct keystore file must always be present in the keystore directory when using an initialized board. If the keystore file is not available, the board must be zeroized and initialized with a new keystore. Once the problem has been corrected, it must be reported to the `fmd` with the `fmadm repair` command to prevent it from being diagnosed each time `fmd` is restarted.

fmd Problems Replayed After Reboot or Restarting fmd

When problems are detected and reported to the Solaris Fault Manager Daemon (fmd) they are correctly diagnosed and logged to syslog. However until these problems are reported as repaired with the fmadm repair command, they are diagnosed and logged to syslog by fmd every time the system is rebooted or fmd is restarted. These messages are misleading because they reflect the diagnosis of past problems, not new ones.

Workaround: Use the fmdump -e command to ensure problems diagnosed are the result of a new problem. When a problem is fixed, it must be reported with the fmadm repair command.

Bug ID 6230578 Large Keystore Size Could Cause vca Operations to Fail

If too many keys are added to a keystore, the keystore size could exceed the available memory on the board. If this occurs, the vca driver is unable to upload or download the keystore to the board and error messages similar to the following are displayed:

```
Feb 17 15:15:09 lattice vca: [ID 598662 kern.warning] WARNING: vca1: Unable to
retrieve keystore from device.
Feb 17 15:15:09 lattice vca: [ID 732820 kern.warning] WARNING: vca1: Unable to
update keystore
Feb 17 15:15:19 lattice vca: [ID 529797 kern.warning] WARNING: vca1: Firmware
did not accept keystore.
Feb 17 15:15:19 lattice vca: [ID 124458 kern.warning] WARNING: vca1: Is the
keystore file corrupt, or the master key invalid?
```

Workaround: If possible, reset the board with the vcaadm utility. If you are unable to use vcaadm, stop all cryptographic operations and use the vcadiag utility.

Note – You must stop all cryptographic operations that use the board before using the vcadiag utility. Failure to do this could cause additional failures.

After the board is reset, remove any unnecessary keys from the keystore to reduce the size.

Known Issues With Sun ONE Web Servers

Bug ID 4532645 Administration Server Messages

If you are running the Sun ONE 4.x or 6.x Administration Server and the Web Server being managed is not running, there are several situations where dialog boxes asking for token passwords are displayed. If very large fonts are used or if there are many tokens (and consequently many Enter password: lines) the buttons on the panel bottom are not displayed because the fixed size dialog box is too small. It is impossible to select the Accept button on the bottom of the panel to submit the change because the dialog box is not resizable.

There are two workarounds for this problem:

- Start the web server first from the command line or from the administration window with the GUI Preference set to On/Off.
- Apply the configuration without starting up the server: Apply→Load Configuration Files.

Bug ID 4532941 and 4593111 Multiple Keystores

Sun ONE Web Servers have difficulty working with configurations where more than one keystore exists. This issue is fixed in Sun ONE Web Server 6.0 Service Pack 5 (SP5).

Workaround: Configure no more than one keystore for all web server instances. You may then configure a different keystore user for each web server instance. This will keep keys for each web server instance separate from one another.

Bug ID 4620283 `pk12util` Utility

The Sun ONE provided utility, `pk12util`, exports certificates and keys from internal software databases and imports them to external hardware databases. However, the `pk12util` utility cannot export certificates or keys from an external hardware database, such as the Sun Crypto Accelerator board:.

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export.  Private Key
could not be located and exported.
```

Bug ID 4607112 Cipher Default Settings

In configuring Sun ONE Web Server 6.0, after selecting the Cipher Default settings, selecting the certificate, selecting the OK button and selecting the Apply link in the far upper right corner to apply the ciphers, the *username:password* entry may be removed if the steps are not executed in the exact order as prescribed in the *Sun Crypto Accelerator 4000 Board Installation and User's Guide*. This issue is fixed in Sun ONE Web Server 6.0 Service Pack 3 (SP3).

This entry is required for the web server to start up correctly with the Sun Crypto Accelerator 4000 board. You may see this when steps are executed in the following order:

1. Select Cipher Default, SSL2 ciphers, or SSL3 ciphers
2. Select OK
3. Select Apply
4. Select Load Configuration

If you think you have executed these steps and the web server does not start up correctly, use the following workaround:

- Edit the file:

```
/usr/iplanet/servers/https-hostname.domain/config/server.xml
```

- Find the line starting with:

```
<SSLPARAMS servercertnickname="Server-Cert". . .
```

- Insert the text *keystore-name*: prior to the text `Server-Cert` in the line, so that the changed line is as follows:

```
<SSLPARAMS servercertnickname="keystore_name:Server-Cert". . .
```

- Restart the web server.

Known Issues With Solaris Cryptographic Framework

Bug ID 6211857 Unloading the `vca` Driver While Running Heavy Cryptographic Traffic

The Solaris Cryptographic Framework does not hold a reference counter on a context while it is in use. When a driver is unloaded/detached, the Solaris Cryptographic Framework frees the context assuming that it is not in use. This causes double deletion on the context and causes panic.

Bug ID 6195428 "Slot Info is NULL for `vca0`" Error

`vcatest` could fail on the first pass when performed on a Sun Fire 15K with error messages similar to the following:

```
# vcatest -p 0 -scvf -o tl=DES+3DES+MD5+SHA1+RSA+DSA+RNG,dev=vca0
11/10/04 17:07:58 venus-a SunVTS6.0build71: VTSID 0
vcatest.VERBOSE vca0:
"Started."
Functional test complete
11/10/04 17:07:58 venus-a SunVTS6.0build71: VTSID 8066 vcatest.
FATAL vca0: "Slot Info is NULL for vca0"
```

When a hardware provider, such as the Sun Crypto Accelerator, unregisters from the kEF (Solaris Cryptographic Framework), the kEF fails to remove the provider entry from the provider tables when some cryptographic operations are scheduled on the provider.

The provider table size is hardcoded to be 512, and when reloading of the driver happens more than 512 times, it might fill up the provider table and make the driver unloadable. With SunVTS, the symptom is the Slot Info being NULL. With other applications, the Venus slot is simply not seen.

Bug ID 6222467 `solaris-crypto pkcs11`

System calls from `C_Initialize`() get interruped.

Bug ID 6222458 `solaris-crypto kcfd`

Multiple calls to `C_Initialize`() lead to ELF messages on the console.

Known Issue With SunVTS

Bug ID 4836099 SunVTS `netlbtest` Internal Fails Without a Loopback Cable

Sun Crypto Accelerator 4000 MMF boards could fail the internal loopback test of the SunVTS test, `netlbtest`. The following error messages might occur:

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbtest.
  FATAL vca1:    "Failed to get the link up.
  Probable_Cause(s):
    (1)Loopback cable not connected.
    (2)Faulty loopback cable.
  Recommended_Action(s):
    (1)Check and replace, if necessary, the loopback cable.
    (2)If problem persists, call your authorized Sun service
provider.
```

These messages can be ignored.

Workaround: Perform SunVTS internal loopback tests with a loopback cable attached.

Known Issues With Specific Platforms

Slot Requirements for the Sun Fire 15K Platform

The Sun Crypto Accelerator 4000 board is supported in 66 MHz slots only on the Sun Fire 15K platform.

Bug ID 6223119 Performing at 33 MHz in a 66 MHz Shared Slot on Sun Fire V890 Systems

In Sun FIre V890 systems, the board performs at 33 MHz in a 66 MHz slot when shared with another board. The board performs at 66 MHz if no other board is on the shared bus. A Sun Crypto Accelerator 4000 board or a Quad Gigabit Ethernet (QGE) board in the shared slot forces both boards into 33 MHz mode.

Bug ID 6224057 Reset Required After Unloading `vca` Driver on Sun Blade 100 Systems

On some Sun Blade 100 systems the Sun Crypto Accelerator 4000 board might require a reset after unloading and loading the `vca` driver. Particularly, this problem might occur when driver packages are removed and replaced with newer packages. This is not an issue because the driver performs an automatic reset of the board when the problem is detected. Messages similar to the following can be ignored when loading and unloading the driver on Sun Blade 100 systems.

```
Jan 25 16:26:13 nspgqa116a vca: WARNING: vca0: Timed out enabling CSR window,
state = 2
Jan 25 16:26:13 nspgqa116a vca: NOTICE: vca0: Failed enabling CSR window,
attempting to reset device
Jan 25 16:26:13 nspgqa116a vca: NOTICE: vca0: Resetting board...
```

Using Sun Metaslot With Sun ONE Applications

SSLv3 Mechanisms Must be Disabled in Sun Metaslot Before Use With the Board.

Sun Metaslot does not perform well with the board when running Sun ONE applications. To use Sun Metaslot with a Sun Crypto Accelerator keystore, disable the SSLv3 mechanisms to enable good performance. To use the Sun Crypto Accelerator keystore slot directly, you do not need to disable them.

Use the following command to disable the `CKM_SSL3_PRE_MASTER_KEY_GEN`, `CKM_SSL3_MASTER_KEY_DERIVE`, `CKM_SSL3_KEY_AND_MAC_DERIVE`, `CKM_SSL3_MASTER_KEY_DERIVE_DH`, `CKM_SSL3_MD5_MAC`, and `CKM_SSL3_SHA1_MAC` mechanisms in the Sun Metaslot.

Note – Note that these are all on one line. You must be superuser to execute this command.

```
% cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
mechanism=CKM_SSL3_PRE_MASTER_KEY_GEN,CKM_SSL3_MASTER_KEY_DERIVE,
CKM_SSL3_KEY_AND_MAC_DERIVE,CKM_SSL3_MASTER_KEY_DERIVE_DH,CKM_SSL3_MD5_MAC,CKM
_SSL3_SHA1_MAC
```

Bug ID 6241300 Using Apache With Metaslot

Because of how Diffie Hellman related ciper suites are implemented in OpenSSL, using Apache with metaslot could cause poor performance and significant CPU idling on the server.

The default cipher suite, EDH-RSA-DES-CBC3-SHA, and all Diffie Hellman related cipher suites can cause this problem.

Workaround: Modify the SSLCipherSuite line in the `/etc/apache/httpd.conf` file to exclude Diffie Hellman related cipher suites as follows:

```
SSLCipherSuite
ALL:!ADH:!EXPORT56:-AES256-SHA:-DHE-RSA-AES256-SHA:-DHE-DSS-AES256-
SHA:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL:-EDH-RSA-DES-CBC3-SHA
```

Bug ID 6190335 Enabling Metaslot Per Process

Metaslot, when enabled system-wide, can be controlled on a per-process basis by setting the environment variable `${METASLOT_ENABLED}` to true or false.

To set an environment variable for SunONE Administration Server programs, add the following line to the `https-admserv/config/magnus.conf` configuration file:

```
Init fn="init-cgi" <ENV_VAR>=<value>
```

The following is an example of disabling metaslot for the process.

```
Init fn="init-cgi" METASLOT_ENABLED="false"
```

Refer to the documentation available at:

`http://docs.sun.com/source/817-6252/npgmagns.html#wp25400`